[38] Directory Structure on the Monitoring System Server:

B1

$VPNLOGS/vpnlogs-<collector process pid>-<sequenctial counter>/<probe hostname>/<vpn name>

[39] File Characteristics: ASCII, colon delimited fields, compressed with gzip, lines beginning with "#" are comment fields, All timestamps are UTC, a "$" character is output on the last line to terminate the file.

[40] The file contents and data structure saved in memory of each record saved in the VPN probing router is as follows:--;

Pages 13-19, mis-numbered paragraphs [1]-[21], substitute therefor:

---

[41] The probing routers may generate SNMP Traps when the number of packets lost in a predetermined amount of time exceeds a predetermined threshold, and if the probe latency is measured as exceeding a predetermined time.

[42] SLA statistical data compiled by the probe poller processor 223 is provided to the SLA reporting system 225. The SLA reporting system 225 provides to a customer a condensed aggregation of data collected by the probe poller processor 223 so that the customer may review whether the SLA was complied with during the reporting interval. In one embodiment, the SLA system 225 aggregates the data on a month-by-month basis and provides the data via a server on an Internet web-site for review by customers of the VPN. Alternatively, a computer and printer are employed to provide written reports summarizing the SLA statistics that were collected for the customer of the VPN.

B2

[43] The probing operations are performed on the network 217 at layer 3 (i.e., IP layer). Thus, the operation is performed independent of the physical and data link layers and thus may be used in any one of a variety of different network configurations such as frame relay, ATM, FDDI, packet-over SONET, Ethernet, fibre channel as well as others. A description of example network systems that may be employed with the current invention is provided in "Data and Computer Communications", by William Stallings, Fifth Ed., Prentice Hall, Chapter pages 401-458, 1997,

the entire contents of which being incorporated herein by reference. Furthermore, Chapters 15 and 16 provide further description of specific protocols and architectures that may be employed with the present invention, and thus Chapters 15-16, pages 497-584 are also incorporated herein by reference.

[44] While encryption may be employed to improve information privacy, encryption need not be employed and thus is an optional feature, selected by a customer when subscribing to the VPN service. The source VPN probing router 207 may also employ multi-protocol label switching that prioritizes packets through the core communication network 217.

[45] Figure 3a illustrates a generic protocol data unit for a probe message sent by the source VPN probing router 207 according to the present invention. Consistent with the operation of TCP/IP, IP header 301a and IP data area 301b form part of an IP datagram portion of a network-level packet 303. The network-level packet 303 includes a frame header 303a and a frame data area 303b.

[46] Figure 3b shows a functional description (i.e., those data fields that are relevant to the present probing discussion) of an IP datagram portion of the packet employed for the probe message. IP header 301a is followed by a source time stamp 321b, which is placed in the IP data area portion of the IP datagram 321. This source time stamp T1 is transmitted in the probe message to the destination VPN probing router 203. Alternatively, the source VPN probing router does not include the time stamp T1, but does save the time stamp in memory for later use after the reply probe message is received.

[47] Figure 3c shows the IP datagram for the reply probe message. As shown, the IP datagram 331 includes a field 331a that holds a measurement value (an indicator) of the remote latency R_L as being equal to $R_2 - R_1$, where R_2 is the time that the destination VPN probing router sent the reply probe message, and R_1 is the time at which the probe message was received by the destination VPN probing router 203. Accordingly, the remote latency R_L is the difference between these two times and measures the amount of time that was required by the destination VPN probing router 203 to generate and send the reply probe message after receiving the probe message. The reply probe message also includes the source time stamp T1 321b. The source probing router 207 then receives the reply probe message at time T2.

[48] Figure 4 represents the internal components of a source VPN probing router according to the present invention. Within a housing 401, the probing router includes a data bus 403 that

interconnects a processor 405 with other components connected to the bus 403. In particular, the processor 405 executes computer readable instructions saved on ROM 409 to implement both a routing engine 477 as well as the programmable probe device 407.

[49] The main memory 408 is a RAM that receives software settable parameters sent from the QVPN builder 227 (Fig. 2) for setting the probing parameters that would be executed by the programmable probe device 407. The programmable probe device 407 is shown to be internal to the processor 405, which is the case when it is implemented only in software, but may also be a separate component that communications with the other components by the bus, or other signal relaying mechanism, such as a local bus or optical link. The programmable probe device includes a timer that generates a probe message after a predetermined time has elapsed since the last probe message was sent. The programmable probe device 407 either maintains internally thereto, or retrieves from main memory 408, a polling interval parameter that was set by the QVPN builder 227. Furthermore, the programmable probe device 407 also receives an indication from the QVPN builder 227 which destination VPN probing routers the source VPN is to communicate with so that tunnels may be established therebetween.

[50] A storage device 410 is also a RAM and is used to hold information regarding round trip delay and whether packets are dropped. This information is later sent to the probe poller processor 223, either on demand from the probe poller processor 223 or at periodic intervals as a software settable parameter and saved in main memory 408. The packet grouping logic 417 and envelope packet logic 419 cooperate to form IP packets for assessing whether received packets are to be routed to a device connected to the router, or not. Likewise, the packet grouping logic 417 and envelope packet logic 419 cooperate to form packets for sending over the IP network 417 by way of the input/output unit 415. A buffer unit 413 serves as a buffer for saving and holding message traffic when the processor 405 is busy (for inbound messages) or for sending packets when either the input/output unit 415 is busy or the IP network 417 is busy. The input/output 415 connects by way of a bus 421 to the IP network 417. A local source terminal 450 also connects to the input/output unit 415 for local accessibility to the router. The IP network 417 and source terminal 450 connect through ports (or connectors) to the housing 401.

[51] Figure 5 is a flowchart showing a process flow for collecting SLA statistics over the VPN. The process begins in step 501 where an inquiry is made regarding whether a predetermined time period has elapsed since the source VPN probing router has sent the last probe message. If the

response to the inquiry is negative, the inquiry is made again until the time period has in fact elapsed. Once the response to the inquiry is affirmative, the process proceeds to step 503 where the source VPN probing router sends a polling packet to the destination VPN probing router 203. The polling packet (probe message) optionally includes a time stamp T1 therein. Alternatively, the source VPN probing router simply stores in memory the time at which the polling packet has been sent, thus not notifying the destination VPN probing router when the message was in fact sent.

[52] After step 503, the process proceeds to step 505 where the probe message is received at a time R_1 at the destination VPN probing router. The destination VPN probing router then prepares a reply probe message and sends the reply probe message at a time R_2 such that the remote latency (i.e., turn-around time of the destination VPN probing router) is given by $R_L = R_2 - R_1$. The process then proceeds to step 507 where the remote latency (or processing delay) R_L is inserted in the reply probe message and the reply probe message is then sent.

[53] After step S507, the process proceeds to step S509 where the programmable probe device 407 (Figure 4) compares the amount of time between when the probe message was sent (T1) and when (if at all) a reply probe message is received (T2). In step 509 if it is determined that the difference between T2 and T1 is greater than a predetermined amount (a software settable parameter) then it is determined that the packet (probe message) was dropped. If the packet was dropped, the process proceeds to step S511 where an indication is saved in memory 410 (Figure 4), or sent directly to the probe poller processor 223 (Figure 2) indicating that a packet was dropped. The process then proceeds to step S519.

[54] If however, the response to the inquiry in step S509 is negative, the process proceeds to step 513 where the time stamp T_2 is determined from when the reply packet (reply probe message) is received and the process then proceeds to step S515 where a round-trip time R_{tt} is calculated. The calculation for round-trip time is determined as $R_{tt} = (T_2 - T_1) - R_L$. The process then proceeds to step S517 where R_{tt} is stored in memory at the probing router, although alternatively the data may be sent directly to the probe poller processor 223 at the VPNOC 221.

[55] The probe poller processor 223 gathers information from the respective probing routers in the VPN and calculates average round-trip time, R_{tt}, availability, and packet loss rate for each tunnel as well as for the entire VPN. After having collected these SLA statistics, the process proceeds to step S521 where an inquiry is made regarding whether an SLA performance is

judged to be below a required level, typically the service level agreement threshold levels. If the response to the inquiry in step 521 is negative, the process repeats so as to maintain a SLA statistical retrieval monitoring process. On the other hand, if the response to the inquiry in step 521 is affirmative, the process proceeds to step 523 where corrective action is taken on the network resources. This may include dispatching a trouble-shooting technician to identify a source of the problem or adjusting the software settable parameters in the probing router, so as to be less stringent on the service level requirements imposed on the network. The corrective action may also include providing a refund to a client, if the service level agreement statistics were in fact below the required level. After step 523 the process then repeats so as to continue the SLA statistic collection and analysis operation.

[56] Figure 6 is a flowchart of a process for automatically and remotely configuring a VPN architecture according to customer-specified requirements. The process begins in step S601 where the QVPN builder 227 is provided with VPN topology configuration information, which identifies the different VPN nodes that will be used in the customer-specified VPN. The process then proceeds to step S603 where the probing routers are either manually assigned a polling interval, or a default setting is included, such as two minute intervals. The process then proceeds to step 605 where the QVPN builder 227 sends configuration messages to the respective probing routers by way of the network 217. The probing routers then set the software settable parameters for the programmable probe device 407 either in the main memory 408 or in the programmable probe device itself.

[57] After step S605 the process proceeds to step S607, where the programmable probe device 407 (Figure 4), causes the SLA statistical data that is saved in the storage device 410 to be sent to the probe poller processor 223 (Figure 2). The probe poller processor 223 creates a database in the probe polling processor and holds the data therein for calculation and distillation of SLA statistical data.

[58] In the event that changes are required in the network, the process proceeds to step 609 where the QVPN builder 227 dispatches a "configuration" message to respective of the programmable probe devices in the probing routers. The configuration messages include the software settable parameters used by the probing routers to determine the polling interval, dropped packet threshold decision time, and other parameters such as particular node addresses to which to communicate with in determining round-trip time for packet transmission. Once the